CLAIMS

1. A card settlement method using a portable electronic device having a fingerprint sensor that connects a portable electronic device having a fingerprint sensor to a card company's card management device via a communication terminal for card settlement of a commodity purchase charge or the like; comprising:

An identity confirmation step wherein said portable electronic device having a fingerprint sensor reads the user's fingerprint using said fingerprint sensor and checks it against pre-registered fingerprint data and thereby confirms whether or not the user is the owner of said portable electronic device having a fingerprint sensor,

A transaction data generation and signature step wherein, when identity is confirmed, said portable electronic device having a fingerprint sensor encrypts commodity order information and pre-registered card information using a pre-registered transmission public key and generates transaction data, and electronically signs it using a pre-registered personal encryption key,

A transmission step wherein said electronically signed transaction data is sent from the side of said portable electronic device having a fingerprint sensor to said card management device, and

A decryption and settlement processing step wherein said card management device decrypts said electronically signed transaction data using a transmission secret key paired with said transmission public key and processes the settlement.

2. A card settlement method using a portable electronic device having a fingerprint sensor according to claim 1, wherein

Said fingerprint data and said card information of said portable electronic device having a fingerprint sensor are registered in a state in which they are encrypted by a storage public key provided from said card management device side, and

The step of decrypting said electronically signed transaction data at said card management device includes a decryption step that uses a storage secret key paired with said storage public key.

3. A card settlement method using a portable electronic device having a fingerprint sensor according to claims 1 or 2, wherein:

Said card management device stores and retains the received said electronically signed transaction data for a predetermined time period.

4. A card settlement method using a portable electronic device having a fingerprint sensor according to claims 1, 2, or 3, wherein:

Said card management device includes a step of updating said transmission public key and said storage public key registered in said portable electronic device having a fingerprint sensor, and

Said portable electronic device having a fingerprint sensor replaces said registered card information and said fingerprint data with said card information and said fingerprint data that was encrypted using said updated storage public key.

5. A portable electronic device having a fingerprint sensor that connects to a card company's card management device via a communication terminal for card settlement of a commodity purchase charge or the like; comprising:

A fingerprint sensor, a storage unit, an external interface for connection to said communication terminal, and a processor for driving and controlling these units,

Said storage unit stores the transmission public key and storage public key provided from said card management device side, card information for card settlement provided to the owner of the portable electronic device having a fingerprint sensor, master fingerprint data, and a personal encryption key,

Said card information and said master fingerprint data are stored in an encrypted state using said storage public key;

Said processor comprises:

A personal encryption key generation means for generating said personal encryption key when said fingerprint sensor reads said master fingerprint data,

An identity confirmation means for confirming identity by comparing a fingerprint read by said fingerprint sensor against said fingerprint data in said storage unit, and

A transaction data generation and transmission means for encrypting commodity order information and said card information using said transmission public key and generating transaction data, for electronic signing using said personal encryption key, and for sending the electronically signed said transaction data to said card management device.

6. A portable electronic device having a fingerprint sensor, used in card settlement, according to claim 5, wherein:

Said processor comprises a master fingerprint data registration means so that when it receives a registration permission signal from said card management device, it reads said master fingerprint data using said fingerprint sensor and registers it, and

Said personal encryption key generation means generates said personal encryption key using the fingerprint data read when reading said master fingerprint data.

7. A card management device for performing card settlement of commodity purchase charges, etc. based on transaction data received via a communication terminal from a portable electronic device having a fingerprint sensor; comprising:

An encryption key generation means for generating a storage public key and a transmission public key provided to said portable electronic device having a fingerprint sensor,

A registration procedure processing means for requesting identity identification information for determining the user when a registration request signal is received from said portable electronic device having a fingerprint sensor, and for sending a registration permission signal to said portable electronic device having a fingerprint sensor when the user is determined based on the received identity identification information,

A decryption means for decrypting said transaction data using a storage secret key paired with said storage public key and a transmission secret key paired with said transmission public key when said encrypted and electronically signed transaction data is received from said portable electronic device having a fingerprint sensor, and

A settlement processing means for processing settlement based on said decrypted transaction data.

8. A card settlement system that connects a portable electronic device having a fingerprint sensor to a card company's card management device via a communication terminal and performs card settlement of commodity purchase charges, etc.; wherein:

Said portable electronic device having a fingerprint sensor comprises:

An identity confirmation means wherein the user's fingerprint is read using said fingerprint sensor and checked against pre-registered fingerprint data, thereby confirming whether or not the user is the owner of said portable electronic device having a fingerprint sensor,

A transaction data generation and signature means wherein, when identity is confirmed, commodity order information and pre-registered card information are encrypted using a pre-registered transmission public key and transaction data is generated, and the transaction data is electronically signed using a pre-registered personal encryption key, and

A transmission means for sending said electronically signed transaction data to said card management device;

Said card management device comprises:

A reception means for receiving said electronically signed transaction data,

A decryption means for decrypting said received electronically signed transaction data using a transmission secret key paired with said transmission public key, and

A settlement processing means for processing settlement based on said decrypted transaction data.

9. A card settlement system that uses a portable electronic device having a fingerprint sensor according to claim 9, wherein:

Said fingerprint data and said card information of said portable electronic device having a fingerprint sensor are registered in a state in which they are encrypted by a storage public key provided from said card management device side, and

Said card management device's decryption means decrypts using a storage secret key paired with said storage public key.

10. A card settlement system that uses a portable electronic device having a fingerprint sensor according to claims 8 or 9, wherein:

Said card management device comprises a storage means for storing and retaining said received transaction data for a predetermined time period.

11. A card settlement system that uses a portable electronic device having a fingerprint sensor according to claims 8, 9, or 10, wherein:

Said card management device comprises an encryption key update means for updating said transmission public key and said storage public key registered in said portable electronic device having a fingerprint sensor, and

Said portable electronic device having a fingerprint sensor comprises a data update means for replacing said registered card information and said fingerprint data with said card information and said fingerprint data that was encrypted using said updated storage public key.